Exhibit 5

technicolor

Security & Content Protection

Video Fingerprinting

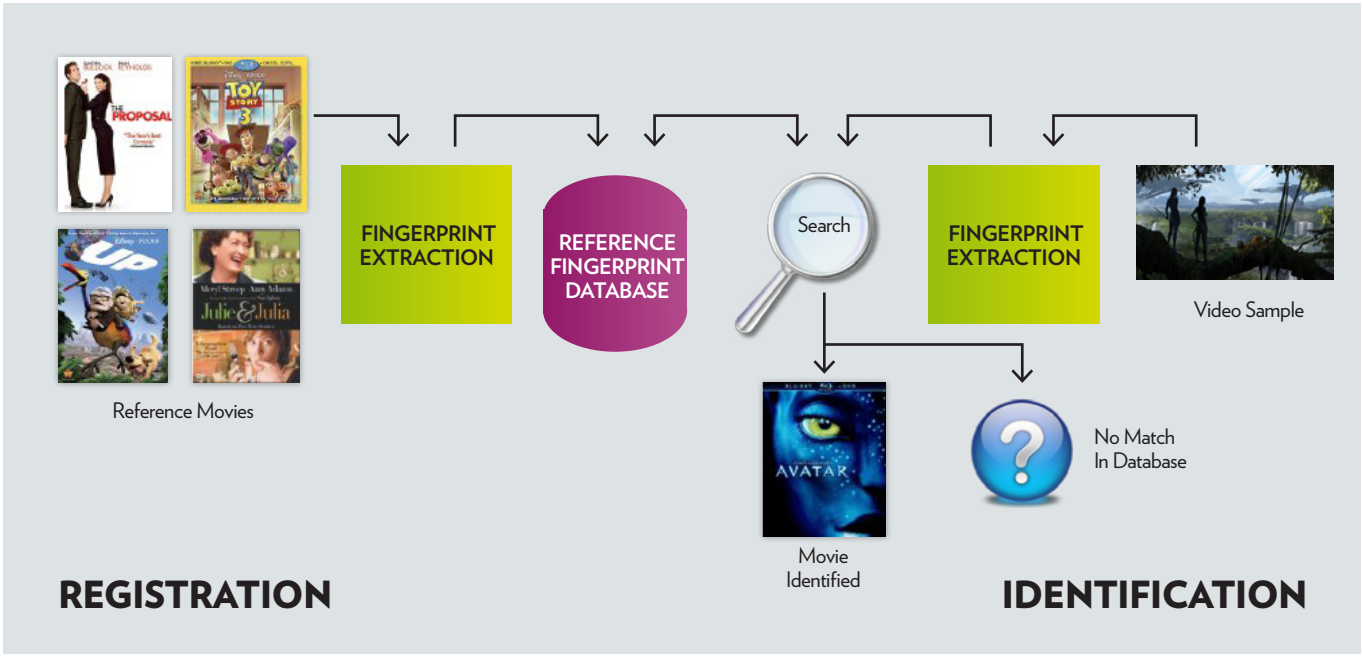
With the ever increasing production of entertainment content, it now became a challenge to easily name a tune or a movie. Digital fingerprinting has been recently introduced to provide a binary identifier which remains stable as long as the content remains perceptually the same. Such technology is much valuable to facilitate content identification. Technicolor's video fingerprinting system can provide a wide range of services, spanning usages from entertainment content enrichment to copyright infringement prevention.

Architecture

A video fingerprinting system typically involves two processes, namely (i) reference movie registration in the fingerprint database and (ii) video query identification.

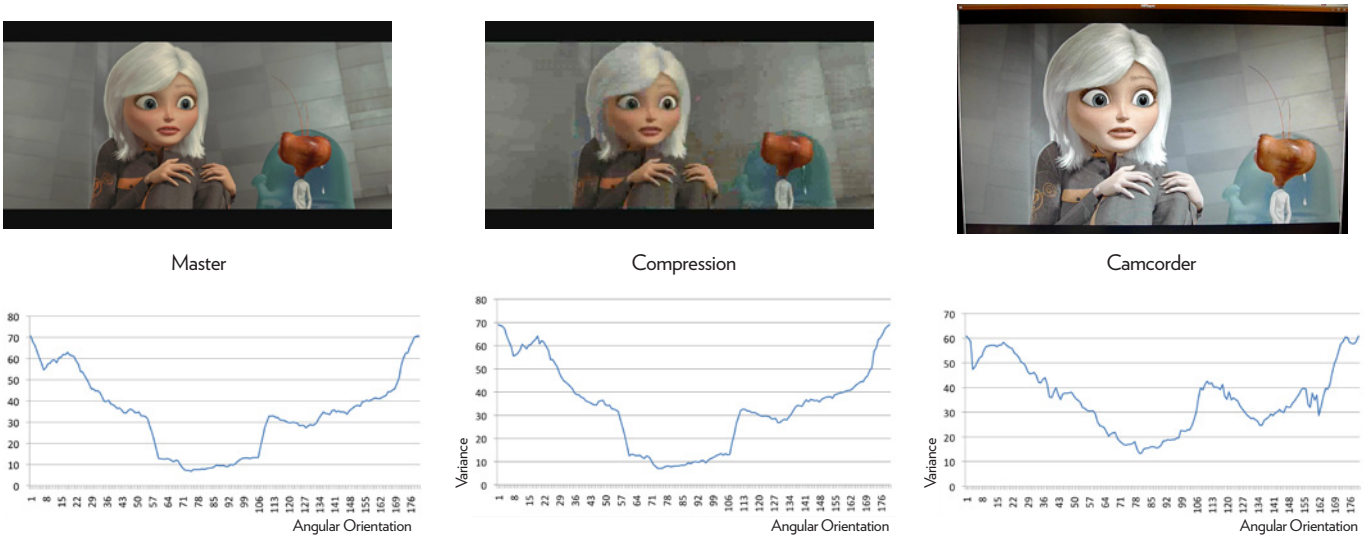
During the registration process, each reference movie is input into the system to compute its identification fingerprint. In contrast with conventional binary identifiers such as cryptographic hash values, modifications preserving the semantics of the content such as lossy compression, filtering, resampling are expected to have a limited impact i.e. most of the fingerprint bits should be preserved. The computed binary fingerprints then populate a reference database.

At a later stage, a video sample, should it be a full movie or only a fragment, is input to the system for identification. The fingerprint of the video is first computed and then used as a query to interrogate the reference database. An elaborate search algorithm is employed to retrieve the registered reference fingerprint which is the closest from the query. This nearest neighbor search is required to mitigate the effects of potential corrupted bits in the query fingerprint. If this is a close match, the tested video is identified as being the one associated to the reference fingerprint. Otherwise, the input video is considered as not being registered in the reference database.



Security & Content Protection

Video Fingerprinting



Technicolor's Security & Content Protection Lab developed a video fingerprinting system which combines three elementary components:

1. **a video frame global descriptor;**
2. **a detector of key frames;**
3. **a video frame local descriptor.**

Radial Hash Function (RASH)

The digest produced by the RASH algorithm basically provides a global description of a video frame. The word "global" indicates that this visual hash function captures high level characteristics of the input video frame but is insensitive to details.

In a nutshell, the RASH algorithm consists in (i) considering the set of pixels belonging to the line passing through the center of the video frame with a specified angular orientation, and (ii) computing some statistics of the luminance value of the selected pixels e.g. the variance. This process is repeated for several orientations, hence resulting in a 180-dimensional visual digest when orientations are discretized by 1°. Regular signal processing primitives barely affect this feature vector; a rotation applied of the video simply results in a shift of the vector which can be compensated for by using cross-correlation.

The RASH algorithm proved to be robust against a wide range of attacks, including resizing, filtering, transcoding, resampling, etc. For illustrative purpose, a couple of visual digests are depicted in the above figure for different versions of a content. Moreover, extensive benchmarking also demonstrated that RASH was discriminating enough to be integrated in a fingerprinting framework and permit movie identification.

Focusing on Key Frames

Keeping in mind that one of the objectives of video fingerprinting is to obtain a compact representation of the movie masters in order to save storage space, it would still be costly to record the RASH digest vector of each and every frame of a movie. As a matter of fact, it is even undesired as it would accumulate in the database similar fingerprints associated to different frames in the movie, therefore possibly confusing the identification process. To alleviate this issue, Technicolor is only storing the RASH digest vectors of the most representative frames of a movie, which are commonly referred to as key frames.

The localization of these key frames is based on the analysis of the dynamics of the RASH digest vectors, and, more precisely, how much/little they differ from one video frame to another. Various studies highlighted the importance of two types of key frames:

- Shot boundary frames corresponding to brutal variations of the visual content e.g. a scene cut introduced by the movie director;
- Shot stable frame corresponding to the frame within a shot with the least temporal activity.

Security & Content Protection

Video Fingerprinting

Both types of key frames can be easily localized by analyzing the distance between the RASH digest vectors of successive video frames. A shot boundary is detected when this distance exceeds a specified threshold. On the other hand, the shot stable frame of a segmented video shot is located at the time index where the RASH digest vector varies the least from one frame to another within this shot. Additional constraints are also considered to avoid selecting extremely bright or dark frames. The key frames localization process is summarized in the graphic below.

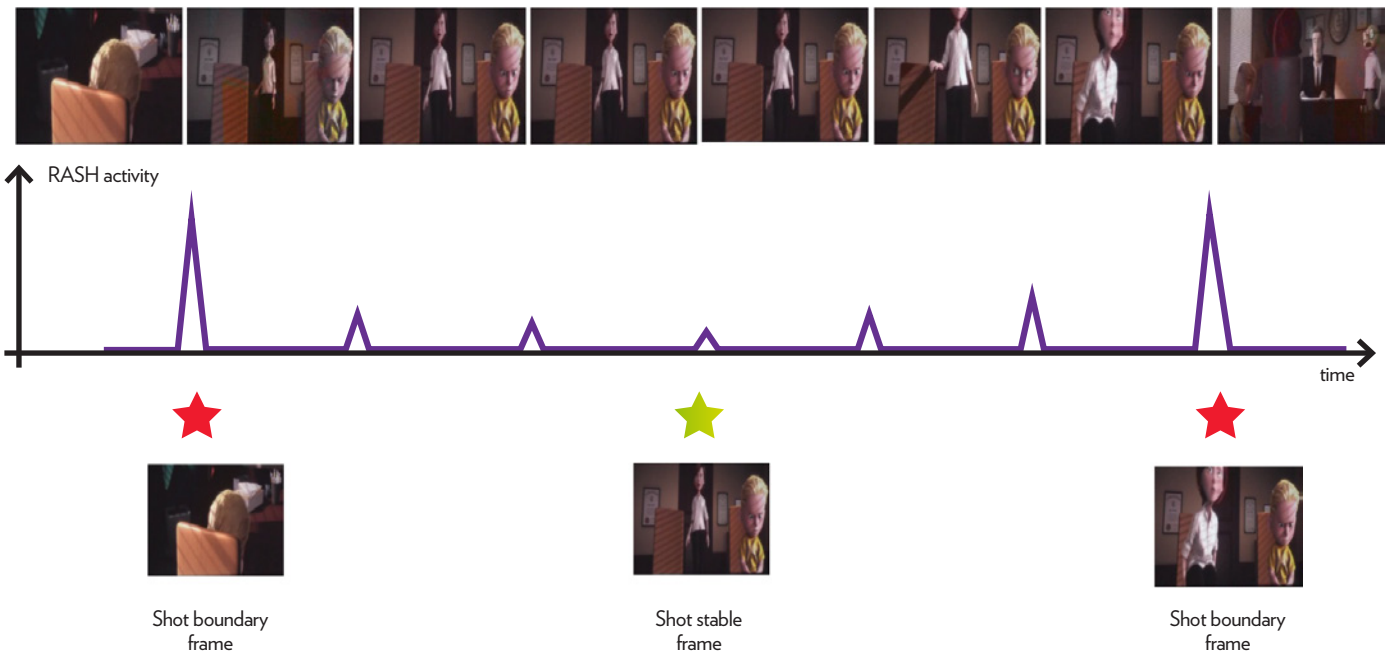
In summary, the fingerprint of a video consists in aggregating the RASH digest vectors of shot boundary frames and stable frames in strict alternation.

Enriching the Fingerprint with Local Information

Similarly to other global descriptors, RASH 'quickly' introduces false positives when populating the database. To mitigate this shortcoming, Technicolor enriches the fingerprint of the key frames with state-of-the-art local descriptors of robust feature points of the key frames. Incorporating information about visual details within the fingerprint permits to preserve the identification capabilities of the fingerprint for much stronger distortions, e.g. camcording, while maintaining the number of false alarms relatively low.

References

- **A. Massoudi, F. Lefèbvre, C.-H. Demarty, L. Oisel, and B. Chupeau**, « A video fingerprint based on visual digest and local fingerprints » , in Proceedings of the IEEE International Conference on Image Processing, pp. 2297-2300, 2006.
- **C. De Roover, C. De Vleeschouwer, F. Lefèbvre, and B. Macq**, « Robust video hashing based on radial projections of key frames », in IEEE Transactions on Signal Processing, 53(10):4020-4037, October 2005.



Security & Content Protection

Video Fingerprinting

Usages

Video fingerprinting enables a wide spectrum of applications ranging from content enrichment to copyright infringement prevention.

Content enrichment: the video fingerprint is used as an index to retrieve relevant information in a relational database e.g. the title of the movie, the names of the actors playing in it, etc.

Localization of copyright content: a crawler browses the Internet and retrieves movie files which are then inspected with video fingerprinting to check whether they are copyrighted or not.

Data Loss Prevention: the video fingerprint is used as a unique identifier to figure out which and where movies are stored and processed. Doing so, it would be possible to log operations in a post-production environment and thus prevent unauthorized operations that may lead to potential leakage.

Copyright infringement prevention: video content uploaded on User Generated Content (UGC) platforms such as YouTube is first inspected using video fingerprinting to prevent unauthorized publication of copyrighted content.

Key Facts at a Glance

- Non-intrusive video identification technology robust both to natural modifications and targeted attacks such as camcording
- Video identification within seconds even in case of crude attacks such as camcording
- Zero false positive
- Detection speed independent of the number of movies registered into the database

TECHNICOLOR WORLDWIDE HEADQUARTERS
1, rue Jeanne d'Arc
92443 Issy-les-Moulineaux France
Tel. : 33 (0) 1 41 86 50 00 - Fax : 33 (0) 1 41 86 58 59

www.technicolor.com

CONTACT
For any question, please contact us at:
Security & Content Protection Lab
Mr. Eric Diehl

eric.diehl@technicolor.com

technicolor